Department of the Interior
Privacy Impact Assessment

August 15, 2014

Name of Project: eMail Enterprise Records and Document Management System (eERDMS)
Bureau: Office of the Secretary
Project's Unique ID: Not Applicable

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street NW, Mail Stop 5547 MIB
Washington, DC 20240
Phone: (202) 208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

No, the eMail Electronic Records and Document Management System (eERDMS) does not contain information on individuals. The eERDMS is a major application that includes four minor applications: Enterprise eArchive System (EES), Enterprise Forms System (EFS), Enterprise Content System (ECS), and Enterprise Dashboard System (EDS). The EES, EFS and ECS components contain personally identifiable information (PII). EDS consists of statistical transactional data and does not contain PII. To ensure privacy implications were addressed for these complex systems, separate privacy impact assessments were conducted on the EES, EFS, ECS, and EDS applications.

a. Is this information identifiable to the individual[1]?
(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These

No, the eERDMS major application does not contain PII on individuals.

b. **Is the information about individual members of the public?** (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

No, the eERDMS major application does not contain PII about members of the public.

c. **Is the information about employees?** (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

No, the eERDMS major application does not contain PII about employees.

2) What is the purpose of the system/application?

The eERDMS is a program which consists of software as a service, and includes four component systems: EES, EFS, ECS, and EDS. These components in eERDMS provide the framework for storing, accessing, and managing the Department's records, regardless of format, media, source, or location. DOI employees will have access to electronic records and documentation through a web browser or mobile device to create, access and share information. As the rate of Information Technology (IT) change accelerates, there are increasing concerns about the government's ability to manage and preserve its records and to meet accountability and archival obligations. Using eERDMS as an enterprise solution allows DOI to address program specific concerns such as preventing the loss of records that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible.

The DOI's overall objective is to identify, acquire and deploy an enterprise application that combines electronic workflow, imaging, and management of documents, e-mails, discovery, and records. To achieve this objective, the DOI has invested in the eERDMS program that provides the framework for enterprise use, storing, accessing, and managing the DOI's records, regardless of format, media, source, or location.

data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

3) What legal authority authorizes the purchase or development of this system/application?

The Department of the Interior, Establishment, 43 U.S.C. 1451; Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 U.S.C. 1401; 43 CFR Public Lands: Interior; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service", April 27, 2011; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments", December 8, 2011; Presidential Memorandum, "Building a 21st Century Digital Government", May 23, 2012; and OMB M-12-18, "Managing Government Records"; 36 CFR 1220: Federal Records, General; Presidential Memorandum, "Managing Government Records", November 28, 2011.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

There is no PII about individuals in the eERDMS major application itself, but eERDMS components do contain PII. The EES, ECS and EFS components of eERDMS contain PII about employees and members of the public. Due to the complexity of these components and the large amounts of PII contained in each, a privacy impact assessment was conducted separately for the EFS, EES, and ECS to ensure appropriate analysis of privacy implications. A separate privacy impact assessment was also conducted on the EDS component, which consists of statistical transactional data and does not contain PII.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The eERDMS major application does not contain PII about individuals. The EFS, EES and ECS components of eERDMS do contain PII, which is obtained from a number of electronic sources including individual employees, members of the public, and other DOI systems. Due to the complexity of the EFS, EES and ECS components and the large amounts of PII contained in each, a privacy impact assessment was conducted separately for the EFS, EES, and ECS to ensure appropriate analysis of privacy implications. A separate privacy impact assessment was also conducted on the EDS component, which consists of statistical transactional data and does not contain PII.

b. What Federal agencies are providing data for use in the system?

The eERDMS is an enterprise-wide program which consists of software as a service, and includes the EES, EFS, ECS, and EDS components. The components in eERDMS provide the framework for storing, accessing, and managing the Department's records, regardless of format, media, source, or location.

Other Federal agencies, employees, or officials who correspond with DOI produce a variety of documents, and provide data and records during the course of conducting official business. These documents, data and records will be captured and maintained in the EES, EFS, ECS, or EDS components of eERDMS. See each component privacy impact assessment for privacy analysis and sources of data.

c. What Tribal, State and local agencies are providing data for use in the system?

Numerous Tribal, State and local agencies interact and partner with DOI and produce a variety of documents, data or records that may be used by DOI and become DOI records. These documents will be stored in various eERDMS components. See each component privacy impact assessment for privacy analysis and sources of data.

d. From what other third party sources will data be collected?

Numerous third parties, such as corporations, charities, and other non-governmental organizations that interact and partner with DOI and produce a variety of documents which may be used by DOI and become DOI records. These documents will be stored in the eERDMS components and may include various types of PII. See each component privacy impact assessment for privacy analysis and sources of data.

e. What information will be collected from the employee and the public?

The eERDMS does not contain PII or collect information directly from employees or members of the public. eERDMS supports the EES, EFS, and ECS components of eERDMS, which do collect and contain large amounts of PII about employees and members of the public. Due to the complexity of these components and the large amounts of PII contained in each, a privacy impact assessment was conducted separately for the EES, EFS, and ECS to ensure appropriate analysis of privacy implications. The EDS component consists of statistical transactional data and does not collect data from employees or the public, nor does it contain PII. See each component privacy impact assessment for privacy analysis and types of data collected from employees and the public.

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOI records be verified for accuracy?**

The eERDMS does not collect, maintain or disseminate PII, or verify records for accuracy. This function is performed by the EES, EFS, ECS and EDS components and varies with each one. See each component privacy impact assessment for privacy analysis on how data is verified for accuracy.

b. **How will data be checked for completeness?**

The eERDMS does not collect, maintain or disseminate PII, or check records for completeness. This function is performed by the EES, EFS, ECS and EDS components and varies with each one. See each component privacy impact assessment for privacy analysis on how data is checked for completeness.

c. **Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The eERDMS is a major application and does not collect, maintain or disseminate PII, or verify that data is current. This function is performed by the EES, EFS, ECS and EDS components and varies for each one. See each component privacy impact assessment for privacy analysis on procedures to ensure data is current.

d. **Are the data elements described in detail and documented?** If yes, what is the name of the document?

Yes, the data elements are described in detail and documented in the eERDMS System Security Plan, standard operating procedures, and other system documentation.

D. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes, eERDMS enables DOI to manage and preserve its records and to meet accountability and archival obligations under the Federal Records Act. Using eERDMS for the enterprise allows DOI to address program specific concerns such as preventing the loss of records that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible.

DOI's overall objective is to identify, acquire and deploy an application that combines electronic workflow, imaging, and management of documents, e-mails, evidence, and records. To achieve this objective, the DOI has invested in the eERDMS program that provides the framework for enterprise use, storing, accessing, and managing the DOI's records, regardless of format, media, source, or location.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No, eERDMS supports the EES, EFS, ECS and EDS components and does not contain PII or create new data about individuals. The privacy implications for new data or data aggregation for the EES, EFS, and ECS components are assessed in separate privacy impact assessments. The EDS does not maintain or file data about individuals and will not collect, use or share any PII about individuals. See each component privacy impact assessment for privacy analysis on data aggregation.

3) Will the new data be placed in the individual's record?

No, eERDMS will not derive new data, create previously unavailable data, or place data in individual records. The privacy implications for how PII data is maintained for the EES, EFS, and ECS components are assessed in separate privacy impact assessments. The EDS will not maintain or file data about individuals and will not collect, use or share any PII about individuals. The EDS system is not designed to and does not derive new data or create previously unavailable data about individuals through aggregation from the information collected. See each component privacy impact assessment for privacy analysis on data aggregation.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No, eERDMS will not make determinations about employees or the public. It is a major application that supports the EES, EFS, ECS and EDS components. Privacy implications are assessed in separate privacy impact assessments for these components. See each component privacy impact assessment for privacy analysis on privacy implications for employees and the public.

5) **How will the new data be verified for relevance and accuracy?**

Not applicable as the eERDMS does not contain information about individuals. eERDMS is a major application that supports the EES, EFS, ECS and EDS components. See each component privacy impact assessment for privacy analysis on data accuracy about individuals.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Not applicable as data is not being consolidated in eERDMS. However, privacy and security controls are implemented to ensure system security and prevent unauthorized access or use. System access is granted only to authorized personnel on an official need to know basis. Only authorized users who have been issued usernames and passwords for each component will be able to access them. In addition, audit features record all actions by users of the system. All personnel must consent to DOI Rules of Behavior and complete annual security, privacy and records management training prior to being granted access to eERDMS or any component.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

Not applicable as processes are not being consolidated in eERDMS. However, privacy and security controls are implemented to ensure system security. User access rights are highly compartmentalized and system access is granted only to authorized personnel on an official need to know basis. Only authorized users who have been issued usernames and passwords for each component will be able to access them. In addition, audit features record all actions by users of the system. All personnel must consent to DOI Rules of Behavior and complete annual security, privacy and records management training prior to being granted access to eERDMS or any component.

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The eERDMS does not contain, collect, maintain, disseminate, or retrieve PII. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis on privacy implications for data collected, stored and retrieved on individuals.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The eERDMS does not maintain PII and does not generate reports on individuals. Audit reports can be produced to review the system access and actions of authorized system users to determine appropriate uses of eERDMS in accordance with all policies and rules for the system.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

The eERDMS is a major application and does not collect, contain, maintain or disseminate PII on individuals. The eERDMS and its components use audit features to ensure appropriate access and use, and authorized system users consent to monitoring prior to accessing DOI networks or systems and must consent to the DOI security banner for the DOI security policy regarding monitoring of network communications. Additionally, all users are required to complete mandatory annual DOI Federal Information System Security Awareness, Privacy and Records Management training prior to obtaining login credentials. Consenting to the Rules of Behavior and the DOI security policy is voluntary; however, personnel who do not consent will not be able to gain access to DOI network resources or information systems. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications and individual consent to the provision of information and the use of that information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The eERDMS is maintained at two vendor locations to provide continuity of service. The primary site will be mirrored to a secondary site for backup purposes or to provide coverage in the event of a significant outage of the primary system. Absent a significant outage, all data transfer will be unidirectional from the primary site to the backup site, and additional data collection will not normally occur at the backup site. As a result, the data in each location will be consistent. In the event that the backup site is used to run the system during an extended outage period, specific automated controls are in place to ensure the complete transfer of all collected data back to the primary site.

2) **What are the retention periods of data in this system?**

Retention periods for records generated by eERDMS or any of the components vary according to agency needs and specific subject matter, and are retained in accordance with applicable Departmental, bureau or office records retention schedules, as approved by the National Archives and Records Administration (NARA). Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor. System administrator logs are covered by NARA's General Records Schedule 20(1)(c). See privacy impact assessments for the EES, EFS, ECS and EDS components for specific records retention periods.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Departmental Manual 1 and NARA guidelines.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes. The eERDMS initiative is the first enterprise-wide web-based system to electronically collect, store and maintain all of DOI's email, records and forms, and it represents a significant technological shift for DOI. The EES, EFS, ECS, and EDS components in eERDMS provide the framework for storing, accessing, and managing the Department's records, regardless of format, media, source, or location. DOI employees will have access to electronic records and documentation through a web browser or mobile device to create, access and share information.

5) How does the use of this technology affect public/employee privacy?

There are privacy implications related to use of cloud based systems. The eERDMS is hosted within a Federal Information Security Management Act (FISMA) moderate environment by a cloud provider. The FISMA environment complies with the National Institute of Standards and Technology (NIST) Special Public (SP) 800-53 control standards so security and privacy concerns have been evaluated, and protocols and procedures for federal cloud applications have been addressed.

Other privacy risks include unauthorized disclosure and misuse of the data in the system. These risks are addressed and mitigated through a variety of administrative and logical security controls. User access is granted only to authorized individuals by system administrators and users are granted access only to the data sets needed in order to perform their job duties; data set access is also governed and limited by the each user's email domain. Individual access is controlled by user-specific passwords. Administrative access to the system is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In many cases, administrators can be granted adequate rights to fulfill their duties without being given access to data in the system.

All users of DOI network resources, including contractors, must consent to DOI Rules of Behavior and take annual security, privacy and records training in order to obtain access to any DOI network resource. System administrators are also required to take computer security role-based training. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications and any affect on public and employee privacy.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

The system generally will not have the potential to identify, locate and monitor individuals. However, the system will have the ability to audit usage of the system, including use by authorized individuals and system administrators. This includes reviewable data concerning logins, including login time. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications related to monitoring of individuals.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

The system is not intended to monitor individuals. However, the system will have the ability to audit usage of the system, including use by authorized individuals and system administrators. This includes reviewable data concerning actions within the system, including username, date and time of day a user accessed the system, specific uniform resource locators (URLs) of component systems, search terms or parameters used to call data, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges. The user traceability program can detect and through ad-hoc capabilities report unauthorized access attempts to files outside of an authorized user’s permissions. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications related to monitoring of individuals.

8) **What controls will be used to prevent unauthorized monitoring?**

The system is not intended to monitor individuals. However, the system will have the ability to audit usage of the system, including reviewable data concerning logins, including login time, to protect against unauthorized access or actions within the system. Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications related to controls to prevent unauthorized monitoring.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

The eERDMS does not collect, maintain or disseminate PII, and is not a Privacy Act system of records. The eERDMS supports the EES, EFS and ECS components, which operate under numerous Government-wide and DOI Privacy Act system of records notices for specific bureau or office programs that collect, process, maintain, or share data, records or forms about individuals. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications and applicable Privacy Act notices. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

The eERDMS is not a Privacy Act system of records. The eERDMS supports the EES, EFS and ECS components, which operate under numerous Government-wide and DOI Privacy Act system of records notices for specific bureau or office programs that collect, process, maintain, or share data, records or forms about individuals. The use of these components by DOI bureaus, offices and programs may require amendment to DOI system of records notices. However, it is the responsibility of each DOI bureau, office or program operating a system of records in an eERDMS component to review their system of records notice for amendments as necessary. See privacy impact assessments for the EES, EFS, ECS and EDS components for analysis of privacy implications and applicable Privacy Act notices. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Access to information will be limited to those authorized individuals that have a need to know the data in order to perform official duties, including system administrators, authorized program personnel, and contractors based on least privileges.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view. Access is further governed by DOI IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to ensure the integrity and protection of information. All DOI employees and contractor employees undergo initial and annual security, privacy and records management training, and sign DOI Rules of Behavior before being granted access to DOI networks and information. See privacy impact assessments for the EES, EFS, ECS and EDS components for specific privacy analysis on data access determinations.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access is restricted to only those individuals authorized by System Administrators on a need to know basis in order to perform their job duties consistent with the purposes of the system. Limitations on access are maintained through user login and authentication. See privacy impact assessments for the EES, EFS, ECS and EDS components for specific privacy analysis on data access restrictions.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view. In addition, firewalls and network security arrangements are built into the architecture of the system and NIST guidelines and Departmental policies are implemented for system and data security. System administrators will monitor the activities of authorized users to ensure that the system is properly used.

Additionally, the system uses a user traceability program that can detect unauthorized access attempts or access to files outside of their permissions. The audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records management training requirement prevent unauthorized access to data, browsing and misuse.

All personnel must consent to DOI Rules of Behavior and complete annual mandatory security, privacy and records management training in order to receive and maintain access to the DOI network or systems.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, contractors were involved with the design and configuration of the system and will be involved with the maintenance and operation of the system. FAR contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (August 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No, eERDMS does not share data or have access to data in other systems. The eERDMS supports the EES, EFS, ECS and EDS components. The EES system integrates with Active Directory (AD) and BisonConnect. AD is used to authenticate and identify users, and BisonConnect is used to journal email from the Google mail platform. See the privacy impact assessments for EES, EFS, ECS and EDS for analysis on how information is accessed and shared with other systems.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The eERDMS system owner and system administrators are responsible for protecting individual privacy rights and will ensure that only authorized DOI and contractor employees can access the system.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

No, other Federal, State, Tribal or local agencies will not share data or have direct access to eERDMS. However, data contained in the EES, EFS, ECS and EDS components may be shared with other agencies as authorized. See the privacy impact assessments for EES, EFS, ECS and EDS for analysis on how information is accessed and shared.

9) How will the data be used by the other agency?

Other agencies will not share data or have access to the eERDMS. Any data shared with or used by other agencies from component systems will be for authorized purposes only. See the privacy impact assessments for EES, EFS, ECS and EDS for analysis on how information is shared or used.

10) Who is responsible for assuring proper use of the data?

The information system owner, system managers, and system administrators are responsible for ensuring the proper use of eERDMS. See the privacy impact assessments for EES, EFS, ECS and EDS for analysis on privacy implications for protecting data privacy.